IFW AF$

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPLICANT(s):	Mikko Lukkaroinen		
SERIAL NO.:	09/525,806	ART UNIT:	2134
FILING DATE:	March 15, 2000	EXAMINER:	Andrew L. Nalven
TITLE:	SECURE USER ACTION REQUEST INDICATOR		
ATTORNEY DOCKET NO.:	490-009156-US(PAR)		

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS BRIEF

(37 C.F.R. §1.192)

This is and appeal from the final rejection of the claims in the subject application. A Notice of Appeal was mailed on February 1, 2005.

I. REAL PARTY IN INTEREST

The real party in interest in this Appeal is the assignee, Nokia Corporation, Helsinki, Finland.

II. RELATED APPEAL AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF THE CLAIMS

Claims 1,2,4 and 5 stand rejected under 35USC103(a) on the basis of the cited reference Holmes, et al, U.S. Patent No. 6,334,056 in view of the disclosure of Wallent et al, U.S. Patent No. 6,366,912. Claims 1,2,4, and 5 are presented for consideration in this appeal and are contained in Exhibit A.

IV. STATUS OF AMENDMENTS FILED SUBSEQUENT TO FINAL REJECTION

During the prosecution of this application, an amendment was filed in response to the final office action mailed May 4, 2005. The amendment submitted therein was not entered by the Examiner. Applicant duly filed a Request for Continuing Examination to obtain consideration of the amendment previously made. The Examiner has issued a first office action rejecting the claims citing the same references. It is from this action that Applicant appeals.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Claims 1 and a claim 4 are amended to make it abundantly clear that the invention sought to be protected in this application is a mobile communications device 1, such as a mobile telephone which is constructed, as shown in figure 2, to determine if inquiries made to the mobile telephone from its communication network are external, i.e. potentially hostile, or internal, i.e. friendly. First and second independent display zones (6,7) are set up in the display screen 5 of the mobile device 1. External inquiries are routed, by means of router 8 only to the first of the displays 6. A confirmation signal may be routed to the second display 7 indicating that an inquiry is internal, while internal communications may be routed to either display 6 or 7. This process is to protect the user of a mobile telephone from bogus inquiries from a server through the mobile communications network.

VI. ISSUES PRESENTED FOR REVIEW

A. The issue presented for review is the propriety of the Examiner's rejection of the claims 1,2,4, and 5 under 35 USC 103(a) based on the cited reference, Holmes, et al, U.S. Patent No. 6,334,056 in view of the disclosure of Wallent et al, U.S. Patent No. 6,366,912. The rejection is contained in the Office Action mailed February 16, 2005. A copy of the cited references are attached as Exhibits B and C.

VII. Argument

With respect to issue A, the examiner has cited the reference Holmes, et al as teaching a control processor for operating a mobile device and a server that teaches sending inquiries for confidential information. The security problem, identified in Holmes, is the concern within an intranet server about breaches incoming from mobile devices, not the reverse as taught in the subject application. This is described in column 2, lines 16-29 as follows:

> **"The intranet may include an interface device which acts as a gateway for communications. Access to the intranet is controlled according to a predetermined criteria. The data gateway may recognize a request from the wireless communications device and routes all communications from these devices through one socket in the gateway to a predetermined interface device, such as an application server. From this interface device, queries may be sent out to the wireless device to enter the appropriate security information for allowing access to the intranet. Once the appropriate information has been entered, and the wireless communication user has been designated as authorized, the interface device directs the requests from the wireless device user to the appropriate applications within the intranet."**

There is no teaching in Holmes of security measures for communications received by a mobile telephone, since the system of Holmes only addresses security breaches coming from remote wireless communications. The examiner characterizes the deficiencies of Holmes as follows:

> **"Holmes fails to teach the ability to identify if inquiries are external or internal and the displaying of the result of the identification on the mobile device display."**

This is a considerable under statement, since Holmes only shows a small liquid crystal display 14 for showing alphanumeric lines of information. There is no mention of static and dynamic displays nor any indication that security information, with respect to inquiries incoming to the mobile telephone, could be displayed.

The Examiner seeks to combine the teaching of Wallent et al with Holmes. Wallent involves a security system for an intranet network in which inquiries are identified by there origin relative to the network firewall. Access to the local area network (intranet) is obtained through a personal computer having a full screen display (figure 7). There is no mention of wireless communications nor any security problems presented thereby. The Examiner refers to first and second displays, while directing attention to the full screen display presented by MICROSOFT INTERNET EXPLORER on a personal computer monitor shown in figure 7. There is no static and dynamic displays, there is only one display with multiple windows distributed over the area of the screen in a well known manner. The only reference to displaying information, in the reference Wallent, that is pertinent is in column 4, lines 48-49 which states, **"During the browsing of a Web site, the browser visually indicates the zone corresponding to the Web site".** This refers to the classification of web sites into security zones having different security precautions. This is viewed from the internet options screen, as shown in figure 3. This system is complex and requires considerably more processing and memory resources than that available on a mobile telephone. It clearly is not applicable to the subject invention.

There is no mention in either of the cited references of security problems caused by interactive applications used on a mobile telephone. Such mobile telephones have no firewalls on which to rely as in the reference Wallent. Applicant submits that the disclosure of Wallent is far afield from the subject invention and bears no relation to the system of Holmes. Neither of the cited references recognize the problem to which the solution of the subject application is directed. Their teachings, therefore, either alone or in combination, do not render the subject invention obvious. The cited reference Wallent does not remedy the deficiencies of the cited reference Holmes.

According to basic tenets of patent law, in order to support an obviousness rejection, there must be some suggestion of the desirability of making the modification, aside from the subject application. The claimed invention must be considered as a whole and the references must suggest the desirability and thus the obviousness of making the modification, the references must be viewed without the benefit of hindsight. (See MPEP sections 706.02(a) and 2141. Applicant submits that the modification of the teachings of Holmes in view of the teachings of Wallent in order to obtain the invention, as described in the claims submitted herein, would not have been obvious to one skilled in the art. The Examiner has failed to present a prima facie issue of obviousness with respect to these claims.

As stated in MPEP Sec. 2142:

> **"To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or**

> **suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria."**

There is no indication that the proposed modification of the referenced systems would be desirable, nor to what purpose such a combination would be made, nor any possibility that some combination of the systems of these references would bear any resemblance to the subject invention.

In spite of the clear and substantial difference between the subject invention and the prior art, the Examiner continued to reject the claims of this application by citing the system (Holmes) for protecting a local area network from incursions into its server generated from mobile telephones. The solution of Holmes is directed to a different problem. It does not teach a system, internal to a mobile communications device, for identifying an inquiry as external or internal and restricting display routing accordingly or directing an indicator symbol to a display, separate from the displayed inquiry.

To this teaching, which does not relate to the internal processing of information within a mobile telephone, the Examiner seeks to combine the disclosure of Wallent, et al. Wallent describes an Internet browser facility for use on a personal computer. It should be noted at the outset, that neither teaching relates to the internal processing of information received in a mobile telephone.

As part of the browser function Wallent provides a means by which Web sites may be classified by the user into security categories, such as "intranet", "trusted", "restricted" and "internet". The "intranet" designation relates to the firewall and to the security of software for the personal computer, "trusted" relates to sites that have been designated by the user as reliable, conversely "restricted" are those that are not reliable. The "Internet" is a generic, unclassified grouping. This system is responsive to the user's security preference selections and designations. The software facility described in Wallent does not support an independent determination of whether an inquiry is internal or external, as in the claims under consideration. It relates to an interactive browser application on a personal computer and is not applicable to a mobile telephone. The software of Wallent would demand extensive processing capability far in excess of anything available in a mobile communications device.

The Examiner continues also to equate windows in a software application to independent passive and dynamic display zones. This is unfounded and applicant submits that the claims of this application define patentable subject matter on this basis alone, since Holmes also does not teach multiple display zones.

Although the browser application of Wallent may be adaptable, in some form, for use in the intranet system of Holmes, no person skilled in the art would recognize the resulting combined system as applicable to a mobile telephone, nor would any feasible combination teach all of the limitations of the claims under consideration. The inquiry into obviousness requires a step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made.

Neither of the references are directed to assisting the security of mobile cell phone usage, in particular with respect to security code inquiries from external sources. The processing capability of a cell phone would be overwhelmed by the demands of the browser of Wallent, not to mention the processing capacity required by the combination with the intranet access system of Holmes.

The combination of teachings relied on by the Examiner do not therefore support the rejection based on obviousness. It would not be obvious to a person skilled in the art that the combined teachings would even relate to the problem addressed in the subject application, much less that such teaching could be combined to obtain the system described in the claims of this application.

VIII. SUMMARY

It is respectfully submitted that all of the claims, as presented, are clearly novel and patentable over the prior art of record. Accordingly, the Board of Appeals is respectfully requested to favorably consider the rejected claims and to reverse the final rejections, thereby enabling this application to issue as a U.S. Letters Patent.

A check in the amount of $500.00 is enclosed for the Appeal Brief Fee. The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

30 MARCH 2005

Geza C. Ziegler, Jr.
Reg. No. 44,004

Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
Telephone: (203) 259-1800
Facsimile: (203) 255-5170

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Board of Patent Appeals and Interferences, United States Patent and Trademark Office, P.O. Box 1450, Alexanderia, VA 22313-1450.

Doris W. Perman

Name of Person Making Deposit

3/31/05

Date

CLAIM APPENDIX

1.(Currently Amended) In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, a system, within said mobile device, for indicating the authenticity of inquiries for confidential identity codes comprising:

a control processor within said mobile device for operating said mobile device, said processor adapted to identify said inquiries for confidential identity codes as externally generated or internally generated;

a display within said mobile device for presenting information to the user, said display divided into first and second discrete display zones; and

routing means within said mobile device constructed to send externally generated information only to said first display zone;

wherein said control processor generates an indication symbol in said second display zone when the inquiry is internally generated to indicate to the user that said inquiry is authentic.

2.(Original) In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, a system within said mobile device for indicating the authenticity of inquiries for confidential identity codes, as described in claim 1, wherein the first and second display zones are dynamic and static displays respectively.

3. (Canceled)

4.(Currently Amended) In a mobile communications device adapted to communicate interactively with a remote network server, said mobile device having a control processor, a user interface and a display, a method for indicating the authenticity of inquiries for confidential identity codes comprising:

internally within the mobile communications device, identifying said inquiries for confidential identity codes as externally generated or internally generated;

internally within the mobile communications device, dividing said display into first and second discrete display zones;

internally within the mobile communications device, routing externally generated inquiries only to said first display zone; and

internally within the mobile communications device, generating an indication symbol in said second display zone when the inquiry is internally generated, to indicate to the user that said inquiry is authentic.

5.(Original) In a mobile communications device adapted to allow a user to communicate interactively with a remote network server, said mobile device having a control processor, a user interface and a display, a method for indicating the authenticity of inquiries for confidential identity codes, as described in claim 4, wherein the first and second display zones are dynamic and static displays respectively.

6. (Canceled)